

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-099428
 (43)Date of publication of application : 07.04.2000

(51)Int.Cl. G06F 13/00
 H04L 12/46
 H04L 12/28
 H04L 12/24
 H04L 12/26
 H04L 12/66
 H04L 29/06
 H04M 3/00

(21)Application number : 10-271092

(71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

(22)Date of filing : 25.09.1998

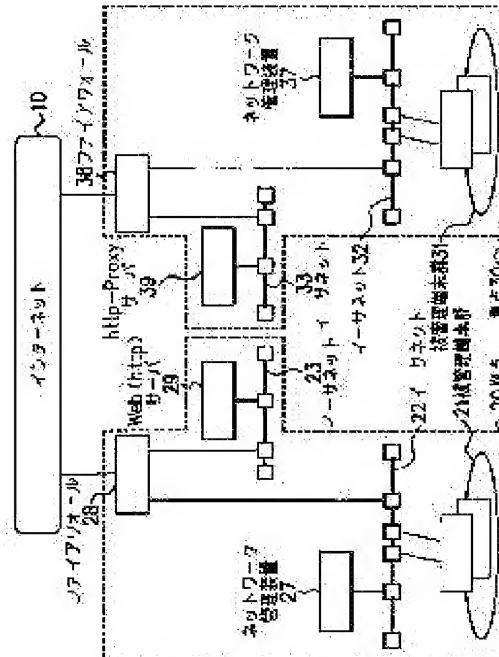
(72)Inventor : NAKAGAWA KENICHI
 NAKAMURA NOBUTAKA

(54) METHOD FOR COLLECTING INFORMATION BETWEEN NETWORKS AND NETWORK MANAGING DEVICE TO BE USED FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for collecting information on one network on the other network without changing any security condition (network policy) and a network managing device to be used for the same.

SOLUTION: A network managing device 37 acquires and stores the equipment or network information of a terminal group 31 to be managed through a managing protocol SNMP, this is assembled into HTTP protocol in order to pass it through a fire wall 38, substitutively transferred to an http-Proxy server 39 and further transferred/stored through an internet 10 into a Web (http) server 29 through an HTTP protocol, and this is acquired with the HTTP protocol by the network managing device 27 and inversely transformed to a managing protocol SNMP so that the equipment or network information of the terminal group 31 to be managed can be provided.



LEGAL STATUS

[Date of request for examination] 23.03.2000

[Date of sending the examiner's decision of rejection] 19.08.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-99428

(P2000-99428A)

(43)公開日 平成12年4月7日 (2000.4.7)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 B 5 B 0 8 9
H 0 4 L 12/46		H 0 4 M 3/00	B 5 K 0 3 0
12/28			D 5 K 0 3 3
12/24		H 0 4 L 11/00	3 1 0 C 5 K 0 3 4
12/26		11/08	5 K 0 5 1

審査請求 未請求 請求項の数 3 O L (全 7 頁) 最終頁に統く

(21)出願番号 特願平10-271092

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(22)出願日 平成10年9月25日 (1998.9.25)

(72)発明者 中川 健一

東京都新宿区西新宿3丁目19番2号 日本
電信電話株式会社内

(72)発明者 中村 信孝

東京都新宿区西新宿3丁目19番2号 日本
電信電話株式会社内

(74)代理人 100069981

弁理士 吉田 精孝

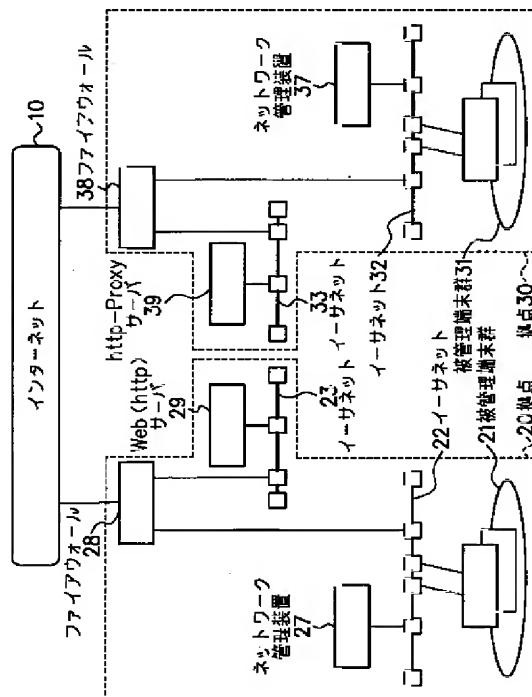
最終頁に統く

(54)【発明の名称】 ネットワーク間における情報の収集方法及びこれに用いるネットワーク管理装置

(57)【要約】

【課題】 セキュリティ条件(ネットワークポリシー)を変更することなく、一のネットワークに関する情報を他のネットワークで収集可能とする方法及びこれに用いるネットワーク管理装置を提供すること。

【解決手段】 ネットワーク管理装置37により被管理端末群31の機器やネットワーク情報を管理プロトコルSNMPで取得し蓄積し、これをファイアウォール38を疎通させるためにHTTPプロトコルに組み立て、http-Proxyサーバ39に代理転送し、さらにインターネット10を介してHTTPプロトコルでWeb(http)サーバ29に転送・蓄積し、これをネットワーク管理装置27によりHTTPプロトコルで取得し、管理プロトコルSNMPに逆変換して被管理端末群31の機器やネットワーク情報を得る。



【特許請求の範囲】

【請求項1】 所定のネットワークポリシーをもって公衆ネットワークに接続される複数のネットワークのネットワーク管理装置間で情報を収集する方法において、ネットワーク管理装置により自ネットワークに関する情報をそのネットワークポリシーの範囲内で自ネットワーク外に転送可能なプロトコルに変換し、公衆ネットワークを介して他のネットワークのネットワーク管理装置に転送することを特徴とするネットワーク間における情報の収集方法。

【請求項2】 変換するプロトコルとしてHTTPプロトコルを用いることを特徴とする請求項1記載のネットワーク間における情報の収集方法。

【請求項3】 請求項1または2記載のネットワーク間における情報の収集方法に使用されるネットワーク管理装置であって、

他のネットワークのネットワーク管理装置に転送する情報を抽出する管理データ抽出手段と、
情報抽出を行う間隔を指示するスケジューリング手段と、
管理データ抽出手段で抽出した情報を自ネットワーク外に転送可能なプロトコルに変換し、かつ他のネットワークから受信した情報のプロトコルを逆変換する転送プロトコル処理手段と、
転送プロトコル処理部とインターフェースとの間でパケットの組立及び分解を行うインターフェース制御手段とを備えたことを特徴とするネットワーク管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、所定のネットワークポリシーをもって公衆ネットワークに接続される複数のネットワークのネットワーク管理装置間で情報を収集する方法及びこれに用いるネットワーク管理装置に関するものである。

【0002】

【従来の技術】図1は従来のネットワーク間における情報の収集方法を用いたシステムの一例を示すもので、図中、1は不特定多数が利用する公衆ネットワーク、2は一のネットワーク管理装置により管理されるネットワークの対象範囲(拠点)、3は他のネットワーク管理装置により管理されるネットワークの対象範囲(拠点)である。

【0003】前記拠点2は、複数の被管理端末からなる被管理端末群21、拠点内の各装置を接続するイーサネット22、23、管理プロトコルを用いて被管理端末群21の管理情報を収集するネットワーク管理装置24、セグメント及びポート単位にパケットの疎通許可禁止等のセキュリティ条件(ネットワークポリシー)を定義可能なファイアウォール25、公衆ネットワーク1等からの情報を蓄積する情報蓄積サーバ26より構成されてい

【0004】また、拠点3は、複数の被管理端末からなる被管理端末群31、拠点内の各装置を接続するイーサネット32、33、管理プロトコルを用いて被管理端末群31の管理情報を収集するネットワーク管理装置34、セグメント及びポート単位にパケットの疎通許可禁止等のセキュリティ条件(ネットワークポリシー)を定義可能なファイアウォール35、イーサネット32、33上の機器と公衆ネットワーク1とのプロトコルを中継するプロトコル中継サーバ36より構成されている。

【0005】図2はファイアウォール25、35のセキュリティ条件により設定されるセグメント間のプロトコル疎通可否について示したもので、横軸の項目はパケットを送出(発信)するセグメント、縦軸の項目はパケットを受信(着信)するセグメントを表している。図中の記号の「○」は発信・着信セグメント間で全プロトコルの疎通を許可し、「×」は全プロトコルの疎通を禁止している。また、「△」は公衆ネットワーク1上の資源を利用するため、必要最低限に限定したプロトコル(HTTP、SMTP、NNTP等)のみの疎通を許可したものであり、内部のネットワークと公衆ネットワーク1との中継を行う。

【0006】詳細に述べると、公衆ネットワーク1から送出されたパケットは、着信側が公衆ネットワーク1の時には全プロトコルの疎通を許可し、イーサネット22、32の時には全プロトコルの疎通を禁止し、イーサネット23、33の時には特定の中継を要するパケットのみ疎通する。

【0007】イーサネット22から送出されたパケットは、着信側がイーサネット22、23の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット23から送出されたパケットは、着信側がイーサネット22、23の時には全プロトコルの疎通を許可し、イーサネット32の時には全プロトコルの疎通を禁止し、公衆ネットワーク1及びイーサネット33に対しては特定の中継を要するパケットのみ疎通する。

【0008】イーサネット32から送出されたパケットは、着信側がイーサネット32、33の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット33から送出されたパケットは、着信側がイーサネット32、33の時には全プロトコルの疎通を許可し、イーサネット22の時には全プロトコルの疎通を禁止し、公衆ネットワーク1及びイーサネット23に対しては特定の中継を要するパケットのみ疎通する。

【0009】

【発明が解決しようとする課題】このような従来の方法では、ネットワーク管理装置24より公衆ネットワーク1を介して拠点3内にある、被管理端末群31やイーサ

ネット32上のネットワーク情報を収集し管理を行う場合、プロトコルが直接疎通可能であることが要求される。そのため、ファイアウォール25、35におけるイーサネット22、32と公衆ネットワーク1との間のセキュリティ条件（ネットワークポリシー）を、全プロトコル疎通禁止から疎通許可に変更する必要があり、新たなセキュリティホールを生じるという問題があった。

【0010】本発明の目的は、ファイアウォール等によって定義されるセキュリティ条件（ネットワークポリシー）を変更することなく、一のネットワークに関する情報を他のネットワークで収集可能とするネットワーク間における情報の収集方法及びこれに用いるネットワーク管理装置を提供することにある。

【0011】

【課題を解決するための手段】本発明では、前記課題を解決する方法として、所定のネットワークポリシーをもって公衆ネットワークに接続される複数のネットワークのネットワーク管理装置間で情報を収集する方法において、ネットワーク管理装置により自ネットワークに関する情報をそのネットワークポリシーの範囲内で自ネットワーク外に転送可能なプロトコルに変換し、公衆ネットワークを介して他のネットワークのネットワーク管理装置に転送することを特徴とする。

【0012】前記構成によれば、一のネットワークに関する情報がそのネットワークポリシーの範囲内で自ネットワーク外に転送可能なプロトコルに変換され、これが公衆ネットワークを介して他のネットワークのネットワーク管理装置に転送されるため、ファイアウォール等によって定義される条件を変更することなく、任意のネットワークの管理情報を収集可能となる。

【0013】この際、変換するプロトコルとしてHTTPプロトコルを用いることができる。

【0014】また、このような方法は、他のネットワークのネットワーク管理装置に転送する情報を抽出する管理データ抽出手段と、情報抽出を行う間隔を指示するスケジューリング手段と、管理データ抽出手段で抽出した情報を自ネットワーク外に転送可能なプロトコルに変換し、かつ他のネットワークから受信した情報のプロトコルを逆変換する転送プロトコル処理手段と、転送プロトコル処理部とインターフェースとの間でパケットの組立及び分解を行うインターフェース制御手段とを備えたネットワーク管理装置を使用することによって実現できる。

【0015】

【発明の実施の形態】図3は本発明のネットワーク間における情報の収集方法の実施の形態の一例を示すもので、図中、従来例と同一構成部分は同一符号をもって表す。即ち、10は不特定多数が利用するネットワークであるインターネット、20は一のネットワーク管理装置により管理されるネットワークの対象範囲（拠点）、30は他のネットワーク管理装置により管理されるネット

ワークの対象範囲（拠点）である。

【0016】前記拠点20は、被管理端末群21、イーサネット22、23、ネットワーク管理装置27、ファイアウォール28、Web(httP)サーバ29より構成されている。また、拠点30は、被管理端末群31、イーサネット32、33、ネットワーク管理装置37、ファイアウォール38、httP-Proxyサーバ39より構成されている。

【0017】ファイアウォール28は拠点20に対するインターネット10からの不正接続を防止し、同拠点のセキュリティを確保する。ファイアウォール38は拠点30に対するインターネット10からの不正接続を防止し、同拠点のセキュリティを確保する。

【0018】図4はファイアウォール28、38のセキュリティ条件により設定されるインターネット及び各イーサネット間のプロトコル疎通可否について示したもので、横軸の項目はパケットを送出（発信）するセグメント、縦軸の項目はパケットを受信（着信）するセグメントを表している。図中の記号の「○」は発信・着信セグメント間で全プロトコルの疎通を許可し、「×」は全プロトコルの疎通を禁止している。また、「△」はHTTPプロトコルの疎通のみを許可し、インターネット10上のWeb参照等のサービス提供を受けることが可能である。

【0019】詳細に述べると、インターネット10から送出されたパケットは、着信側がインターネット10の時には全プロトコルの疎通を許可し、イーサネット22、32の時には全プロトコルの疎通を禁止し、イーサネット23、33の時にはHTTPプロトコルのみ疎通する。

【0020】イーサネット22から送出されたパケットは、着信側がイーサネット22、23の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット23から送出されたパケットは、着信側がイーサネット22、23の時には全プロトコルの疎通を許可し、イーサネット32の時には全プロトコルの疎通を禁止し、インターネット10及びイーサネット33に対してはHTTPプロトコルのみ疎通する。

【0021】イーサネット32から送出されたパケットは、着信側がイーサネット32、33の時には全プロトコルの疎通を許可し、それ以外のセグメントに対しては全プロトコルの疎通を禁止する。イーサネット33から送出されたパケットは、着信側がイーサネット32、33の時には全プロトコルの疎通を許可し、イーサネット22の時には全プロトコルの疎通を禁止し、インターネット10及びイーサネット23に対してはHTTPプロトコルのみ疎通する。

【0022】ネットワーク管理装置37は、拠点30に設置されている被管理端末群31の機器情報やネットワ

ーク管理情報を管理プロトコルSNMPにより収集するとともに、HTTPプロトコルを用いて当該情報を転送する機能を有する。ネットワーク管理装置27は、拠点20に設置されている被管理端末群21の機器情報やネットワーク管理情報を管理プロトコルSNMPにより収集するとともに、HTTPプロトコルを用いてネットワーク管理装置37が収集した機器情報やネットワーク情報を収集し表示する機能を有する。

【0023】Web (http) サーバ29は、ネットワーク管理装置37が収集した情報を蓄積することが可能であり、その接続はHTTPプロトコルによる。http-Proxyサーバ39はイーサネット32上の装置がインターネット10やWeb (http) サーバ29に接続を行うため、HTTPプロトコルのパケットを中継する機能を有する。

【0024】図5はネットワーク管理装置27においてインターネット10を介して被管理端末群31に関する情報を取得する際のシーケンスを示すものである。

【0025】ネットワーク管理装置37は定常的に自管理下にある被管理端末群31の機器やネットワーク情報を管理プロトコルSNMPで取得し、その情報を自装置内に蓄積・格納している。ネットワーク管理装置37は蓄積・格納した情報をファイアウォール38を疎通させるためにHTTPプロトコルに組み立て、http-Proxyサーバ39に代理転送する。

【0026】HTTPプロトコルで情報を受け取ったhttp-Proxyサーバ39は、情報の蓄積先であるWeb (http) サーバ29に対してインターネット10を介してHTTPプロトコルで転送を行う。Web (http) サーバ29は当該情報を所定の場所に蓄積・保管する。

【0027】ネットワーク管理装置27は、HTTPプロトコルでWeb (http) サーバ29に接続を行い、該サーバ29上の所定の場所から情報を取得し、これを管理プロトコルSNMPに逆変換することにより、被管理端末群31の機器やネットワーク情報を得ることができる。

【0028】図6はネットワーク管理装置の詳細構成を示すもので、大別して既存NMS (Network Management System) 機能部40と、NMS連携機能部50とからなり、外部とのインターフェースを介してネットワーク（イーサネット）に接続されている。

【0029】既存NMS機能部40とは、従来より実現されているネットワーク管理機能を実行する部分を示しており、ネットワーク情報表示部41、ネットワーク管理基本部42、管理プロトコル処理部43、インターフェース制御部44より構成されている。

【0030】ネットワーク情報表示部41はネットワーク管理基本部42の情報を画面上に表示する機能を有す

る。ネットワーク管理基本部42はネットワーク上の機器等の構成や状態を監視する機能を有する。管理プロトコル処理部43はネットワーク管理基本部42からネットワーク上の機器等に関する情報の取得依頼を管理プロトコルに翻訳し、または取得依頼に伴う戻り値をネットワーク管理基本部42に送信する機能を有する。インターフェース制御部44は管理プロトコル処理部43とインターフェースとの間でパケットへの組立及び分解を行う機能を有する。

【0031】また、NMS連携機能部50とは、本発明に関わるネットワーク管理機能を実行する部分を示しており、スケジューリング部51、管理データ抽出部52、転送プロトコル処理部53、インターフェース制御部54より構成されている。

【0032】スケジューリング部51は管理データ抽出部52に対して動作を行う間隔を指示する機能を有する。管理データ抽出部52はネットワーク管理基本部42から他のネットワーク管理装置に転送する情報を抽出し、転送プロトコル処理部53へ送信し、また、転送プロトコル処理部53より受信した機器等の情報をネットワーク管理基本部42に送信する機能を有する。転送プロトコル処理部53は管理データ抽出部52から送出された情報を自ネットワーク外へ転送可能なプロトコルに変換し、インターフェース制御部54に送信し、また、インターフェース制御部54より受信した他のネットワークからの情報（管理データ）の転送プロトコルを逆変換する機能を有する。インターフェース制御部54は転送プロトコル処理部53とインターフェースとの間でパケットへの組立及び分解を行う機能を有する。

【0033】

【発明の効果】以上説明したように、本発明によれば、各ネットワークにおけるセキュリティを低下させることなく、任意のネットワークにおける情報をあたかも自管理下のネットワークのように収集することが可能となる。

【図面の簡単な説明】

【図1】従来のネットワーク間における情報の収集方法の一例を示すシステム構成図

【図2】図1中のファイアウォールにおけるネットワークポリシーを示す図

【図3】本発明のネットワーク間における情報の収集方法の実施の形態の一例を示すシステム構成図

【図4】図3中のファイアウォールにおけるネットワークポリシーを示す図

【図5】ネットワーク管理装置27においてインターネット10を介して被管理端末群31に関する情報を取得する際のシーケンスを示す図

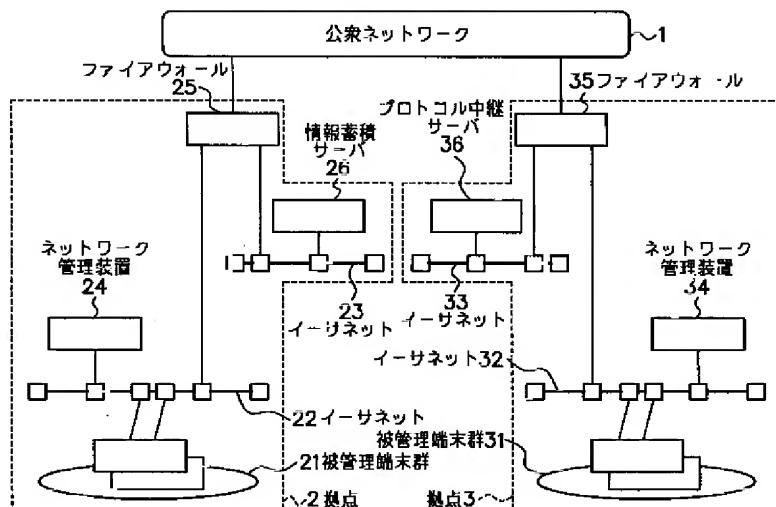
【図6】ネットワーク管理装置の詳細構成を示す機能ブロック図

【符号の説明】

10: インターネット、20, 30: ネットワークの対象範囲(拠点)、21, 31: 被管理端末群、22, 23, 32, 33: イーサネット、27, 37: ネットワーク管理装置、28, 38: ファイアウォール、29: Web (http) サーバ、39: http-Proxy サーバ、40: 既存NMS 機能部 40, 41: ネット

ワーク情報表示部、42: ネットワーク管理基本部、43: 管理プロトコル処理部、44, 54: インタフェース制御部、50: NMS 連携機能部、51: スケジューリング部、52: 管理データ抽出部、53: 転送プロトコル処理部。

【図1】



【図2】

発	公衆ネットワーク1	イーサネット22	イーサネット23	イーサネット32	イーサネット33
公衆ネットワーク1	○	×	△	×	△
イーサネット22	×	○	○	×	×
イーサネット23	△	○	○	×	△
イーサネット32	×	×	×	○	○
イーサネット33	△	×	△	○	○

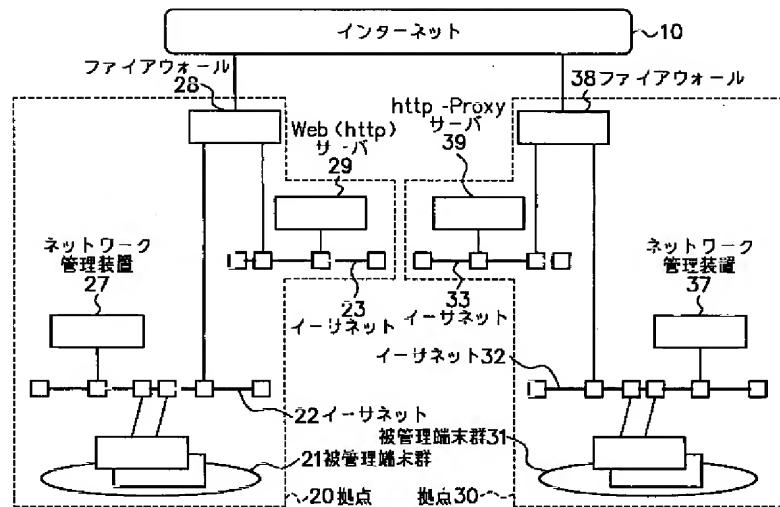
※ ○: 全プロトコル疎通許可, ×: 全プロトコル疎通禁止, △: 特定の中継プロトコル疎通許可

【図4】

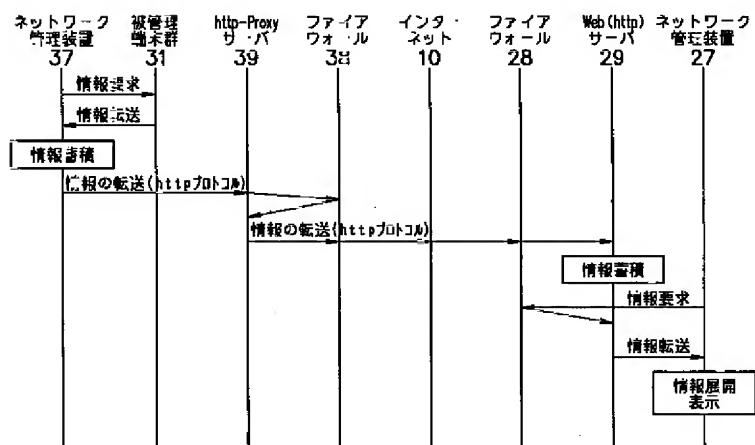
発	インターネット10	イーサネット22	イーサネット23	イーサネット32	イーサネット33
インターネット10	○	×	△	×	△
イーサネット22	×	○	○	×	×
イーサネット23	△	○	○	×	△
イーサネット32	×	×	×	○	○
イーサネット33	△	×	△	○	○

※ ○: 全プロトコル疎通許可, ×: 全プロトコル疎通禁止, △: HTTPプロトコル疎通許可

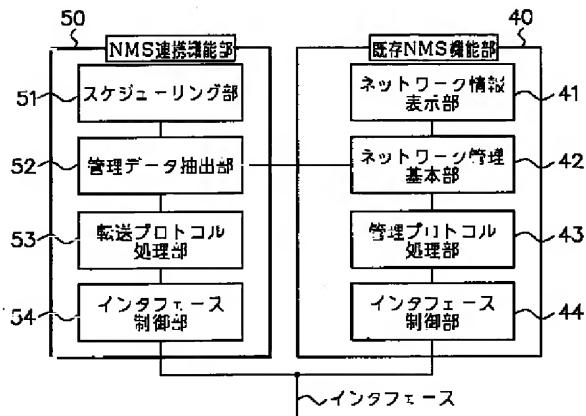
【図3】



【図5】



【図6】



フロントページの続き

(51) Int.C1. ⁷	識別記号	F I	(参考)
H O 4 L	12/66	H O 4 L	
	29/06	11/20	B
H O 4 M	3/00	13/00	3 0 5 C

F ターム(参考) 5B089 GA14 GA19 GA21 GB01 HA01
 HB05 HB06 JA21 KA17 KB13
 KC27 KF05
 5K030 HB06 HC01 HC14 HD08 JA10
 LB15 MC07 MC09
 5K033 BA08 BA11 BA13 CB02 CB08
 CB14 DA01 DA06 DB20 EA07
 5K034 AA13 AA14 EE09 HH61 HH65
 MM89 QQ08 TT02
 5K051 BB02 FF01